

## CLAIMS

1. A data protection management system enabling data communication of a license and encrypted content between a sender and a receiver while protecting and managing the communicated data, the data protection management system comprising:

5 a session manager for executing a process for acquiring a license and encrypted content from a sender;

10 a license management engine for storing and managing the license acquired by the session manager; and memory for storing the license;

15 wherein when a challenge, which is a request for proof of a license, is received, the session manager generates a certificate verifying the license and sends the generated certificate to the receiver.

2. A data protection management system as described in claim 1, further comprising a usage rules administrator for 20 determining usage rules related to the license, and applying the usage rules to processing at least one of the license and content.

3. A data protection management system as described in 25 claim 1, wherein the session manager encrypts the certificate.

4. A data protection management system as described in

claim 1, wherein the session manager adds an optional item from the license to the certificate.

5. A data protection management system as described in  
claim 4, wherein the optional item data is encrypted using a  
key contained in the license.

10. A data protection management system as described in  
claim 2, wherein the usage rules include information for  
determining, based on the license, data to be added to the  
certificate.

15. A data protection management system as described in  
claim 1, wherein the session manager, when a license  
change is received from the sender, reads the license  
before the change from the license management engine,  
changes the license, and saves the changed license in the  
license management engine.

20. A data protection management system as described in  
claim 1, wherein the session manager uses the key to  
decrypt content.

25. A data protection management system as described in  
claim 1, wherein session manager re-encrypts the decrypted  
content.

10. A data protection management system as described in

claim 9, wherein the key used for re-encryption is generated based on information from the sender.

11. A data protection management method enabling data  
5 communication of a license and encrypted content between  
a sender and a receiver while protecting and managing the  
communicated data, the data protection management  
method comprising:

a session step for executing a process for acquiring a  
10 license and encrypted content from a sender;

a step for storing and managing the license acquired  
by the session manager [sic];

a step for storing a key required for decrypting the  
encrypted content; and

15 a step for storing the license;

wherein when a challenge, which is a request for proof  
of a license, is received, the session step generates a  
certificate verifying the license and sends the generated  
certificate to the receiver.

20

12. A data protection management method as described in  
claim 11, further comprising a step for determining usage  
rules related to the license, and a step for applying the  
usage rules to processing at least one of the license and  
25 content.

13. A data protection management method as described in  
claim 11, wherein said session step encrypts the certificate.

14. A data protection management method as described in claim 11, wherein said session step adds an optional item from the license to the certificate.

5

15. A data protection management method as described in claim 14, wherein the optional item data is encrypted using a key contained in the license.

10 16. A data protection management method as described in claim 12, wherein the usage rules includes information for determining, based on the license, data to be added to the certificate.

15 17. A data protection management method as described in claim 11, wherein the session step comprises, when a license change is received from the sender, reading the license before the change from the license management engine, changing the license, and saving the changed 20 license in the license management engine part.

18. A data protection management method as described in claim 11, wherein the session step uses the key to decrypt content.

25

19. A data protection management method as described in claim 18, wherein the session step re-encrypts the decrypted content.

20. A data protection management method as described in  
claim 19, further comprising the step for generating the key  
used for re-encryption based on information from the  
5 sender.